Radboud University

Wedges, oil, and vinegar

A new algorithm for UOV in characteristic 2

Lars Ran

May 6, Rump Session Eurocrypt 2025

A new wedge product-based algorithm

Leverages the fact that the polar forms of the UOV public key in characteristic 2 are alternating

Why should you care?

Scheme	v	o	m	q	o'	Complexity	SL
UOV	68	44	44	2^8	18	*140*	I
	96	64	64	2^4	22	175	I
	112	72	72	2^8	26	*206*	III
	148	96	96	2^8	32	**257**	V
MAYO	64	17	64	2^4	13	**112**	I
SNOVA	74	34	68	2^4	15	**127**	I
	75	24	72	2^4	14	**123**	I
	96	20	80	2^4	19	160	I
	112	50	100	2^4	20	**174**	III
	147	33	99	2^4	31	249	III
	148	32	128	2^4	26	224	III
	120	25	125	2^4	19	**172**	III
	150	66	132	2^4	26	**225**	V
	198	45	135	2^4	40	323	V
	145	30	150	2^4	22	**200**	V

The UOV public map

Central map:

$$f_k(\mathbf{x}) = \sum_{\substack{i \leq n \\ j \leq v}} \alpha_{ij}^{(k)} x_i x_j = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$$

Polar form:

$$\mathbf{F}_k + \mathbf{F}_k^\top = \sum \alpha_{ij}^{(k)} \mathbf{e}_i \wedge \mathbf{e}_j$$

Central map:

$$f_k(\mathbf{x}) = \sum_{\substack{i \leq n \\ j \leq v}} \alpha_{ij}^{(k)} x_i x_j = \mathbf{x}^\top \mathbf{F}_k \mathbf{x}$$

Polar form:

$$\mathbf{F}_k + \mathbf{F}_k^\top = \sum \alpha_{ij}^{(k)} \mathbf{e}_i \wedge \mathbf{e}_j$$

Similarly, with $\{\mathbf{v}_1, \ldots, \mathbf{v}_v\}$ a basis for $O^\perp$, the polar form of the public map $p_k(x)$ is

$$\mathbf{Q}_k = \mathbf{P}_k + \mathbf{P}_k^\top = \sum \beta_{ij}^{(k)} \mathbf{v}_i \wedge \mathbf{e}_j$$

The equations

For $\{\mathbf{v}_1, \ldots, \mathbf{v}_v\}$ a basis for $O^\perp$ we obtain the following equality

$$\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{Q}_k = \sum \beta_{ij}^{(k)} \mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{v}_i \wedge \mathbf{e}_j = \mathbf{0}$$

The equations

For $\{\mathbf{v}_1, \ldots, \mathbf{v}_v\}$ a basis for $O^\perp$ we obtain the following equality

$$\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{Q}_k = \sum \beta_{ij}^{(k)} \mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{v}_i \wedge \mathbf{e}_j = \mathbf{0}$$

And thus we construct a map with $\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v$ in the kernel

$$\begin{aligned} (-) \wedge \mathbf{Q} : \mathbb{F}_q^{\binom{n}{v}} &\to \mathbb{F}_q^{m\binom{n}{v+2}} \\ \mathcal{V} &\mapsto (\mathcal{V} \wedge \mathbf{Q}_1, \ldots, \mathcal{V} \wedge \mathbf{Q}_m) \end{aligned}$$

The equations

For $\{\mathbf{v}_1, \ldots, \mathbf{v}_v\}$ a basis for $O^\perp$ we obtain the following equality

$$\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{Q}_k = \sum \beta_{ij}^{(k)} \mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v \wedge \mathbf{v}_i \wedge \mathbf{e}_j = \mathbf{0}$$

And thus we construct a map with $\mathbf{v}_1 \wedge \ldots \wedge \mathbf{v}_v$ in the kernel

$$\begin{aligned} (-) \wedge \mathbf{Q} : \mathbb{F}_q^{\binom{n}{v}} &\to \mathbb{F}_q^{m\binom{n}{v+2}} \\ \mathcal{V} &\mapsto (\mathcal{V} \wedge \mathbf{Q}_1, \ldots, \mathcal{V} \wedge \mathbf{Q}_m) \end{aligned}$$

If the kernel is of dimension 1, we can find it using sparse linear algebra, and hence retrieve the oil space!

Experimental evidence

Tested the rank prediction for 3188 different (non-trivial) parameter sets (v, o, m)

Only 7 notable exceptions corresponding to $v \geq 2m$

After further analysis these can be accounted for with a single rule

Perfect prediction for all 3188 instances

Thanks for listening!

Scheme	v	o	m	q	o'	Complexity	SL
UOV	68	44	44	2^8	18	140	I
	96	64	64	2^4	22	175	I
	112	72	72	2^8	26	206	III
	148	96	96	2^8	32	257	V
MAYO	64	17	64	2^4	13	112	I
SNOVA	74	34	68	2^4	15	127	I
	75	24	72	2^4	14	123	I
	96	20	80	2^4	19	160	I
	112	50	100	2^4	20	174	III
	147	33	99	2^4	31	249	III
	148	32	128	2^4	26	224	III
	120	25	125	2^4	19	172	III
	150	66	132	2^4	26	225	V
	198	45	135	2^4	40	323	V
	145	30	150	2^4	22	200	V